Symantec™ Advanced Threat Protection: Endpoint

產品型錄：**Advanced Threat Protection**

問題

幾乎現今所有的進階持續性威脅都會利用端點系統來滲透攻擊者鎖定的企業，無論是攻擊漏洞、透過社交工程、網路釣魚網站或上述所有伎倆的組合。一旦入侵受害者的基礎架構，目標式攻擊就會利用端點系統周遊於網路中、竊取憑證及連線至指令與控制 (command-and-control) 伺服器，目的都是為了危害企業最重要的系統與資料。

這個問題只會越來越嚴重。在 2014 年，每六家大型企業 (員工人數超過 2,500 名) 中就有五家成為目標式攻擊的受害者，而超過 60% 的目標式攻擊是針對中小企業發動的。現今的資安方法顯然無法招架，使得位於各地所有規模的企業都暴露在風險中。[1]

解決方案

Symantec™ Advanced Threat Protection: Endpoint 是一套全新的解決方案，可運用您在 Symantec™ Endpoint Protection 的既有投資，橫跨所有的端點發現、排定優先順序及矯正進階攻擊。只要按一下按鈕，就可以搜尋、發現和矯正端點系統中任何攻擊的跡象。同時，如果您還擁有 Symantec™ Advanced Threat Protection: Network 或 Symantec™ 電子郵件安全雲端服務，賽門鐵克的 Synapse™ 交叉比對技術會自動彙總所有賽門鐵克保護的控制點事件，排定您企業中最嚴重威脅的優先順序。

發現進階攻擊並排定其優先順序

Symantec Advanced Threat Protection: Endpoint 結合了來自全球大型網路威脅情報網的全球遙測與本地客戶所有端點的環境，藉此發現原本可能規避偵測的攻擊。

安全分析師可以在單一地點檢視所有的端點攻擊元件，瞭解威脅如何進入企業、受到威脅的電腦清單、該威脅建立了哪些新檔案，以及威脅下載了哪些檔案。分析師也可透過搜尋企業中的所有端點，尋找任何「遭到入侵」的跡象。舉例來說，安全分析師可以讓該產品「顯示具有 BAD.EXE 檔案的所有電腦」或「顯示具有登錄機碼 X、設定 Y 並連線至網站 Z.com 的所有電腦」。而由於 Symantec Advanced Threat Protection: Endpoint 可運用客戶已安裝的 Symantec Endpoint Protection，因此這些功能無需另外安裝新的端點代理程式即可取得。

接下來，Symantec Advanced Threat Protection: Endpoint 會依重要性排定優先順序，讓安全分析師可以密切注意特定的重要端點事件。

1. 賽門鐵克™ 2015 年 4 月出版之第 20 期網路安全威脅研究報告

Symantec Cynic™ 雲端沙箱與 Payload Detonation 服務

Symantec Advanced Protection: Endpoint 客戶可將任何可疑的檔案傳送至 Symantec Cynic，這是一項全新打造的雲端沙箱和 Payload Detonation 服務，可搜尋並排定現今最複雜的目標式攻擊優先處理。Cynic 運用進階的機器學習分析，並結合了賽門鐵克的全球情報，以偵測隱匿和持續性的威脅。Cynic 也可提供客戶每個檔案的功能和它可執行的動作相關細節，讓所有相關的攻擊元件都能快速獲得矯正。現今有 28% 的進階攻擊「可感知虛擬機器」[2]，也就是說這類攻擊在一般的沙箱系統中無法暴露其可疑行為。為了與之對抗，Cynic 也會在實體硬體執行可疑檔案，以發掘原本可規避傳統沙箱技術偵測的攻擊。

Symantec Synapse™ 交叉比對

Symantec Advanced Protection: Endpoint 是整套 Symantec Advanced Threat Protection 產品的一部分，該產品也包括網路和電子郵件端點的模組。賽門鐵克全新的 Synapse 交叉比對技術可彙總所有已安裝控制點的可疑行為，快速辨識和排定遭入侵且需立即矯正的系統之優先順序。

快速矯正

當任何攻擊元件被辨識為惡意攻擊，Advanced Threat Protection: Endpoint 可迅速執行矯正。只要按一下按鍵，客戶就可以快速移除和阻擋攻擊元件針對所有端點發動的進一步攻擊。此產品還提供了攻擊的相關入侵指標 (Indicators-of-Compromise) 的獨特視覺化功能，包括所有入侵指標彼此之間關聯性的完整圖形化檢視畫面。分析師可查看特定攻擊所使用的全部檔案、所有檔案的下載來源 IP 位址、所有安裝的登錄機碼等內容。分析師可依需求按一下按鍵，即可矯正任何端點的任何攻擊元件。

運用現有賽門鐵克投資

Symantec Advanced Threat Protection: Endpoint 會運用並強化您在 Symantec Endpoint Protection 的既有投資，且不需另外部署任何新的端點代理程式。在一小時內，客戶就可以部署全新安裝的 Symantec Advanced Threat Protection: Endpoint 並開始偵測攻擊。該產品也會匯出豐富的情報至第三方的「安全資安事端與事件管理系統」(Security Incident and Event Manager system，簡稱 SIEM)，並傳送如「電腦 A 從網站 C.com 下載了檔案 B.EXE」的資料，而不只是像「已偵測到病毒 BAD.EXE」的傳統安全資料。此外，Symantec Advanced Threat Protection: Endpoint 可由 Symantec™ Managed Security Services 進行監控。

整合檢視橫跨端點、網路和電子郵件的攻擊

Advanced Threat Protection: Endpoint 屬於 Symantec™ Advanced Threat Protection 的一部分；這套統一解決方案可協助客戶發現、排定優先順序並快速矯正現今最複雜的攻擊。它還結合了來自端點、網路和電子郵件的情報，以及賽門鐵克龐大的全球偵測器網路，並且可由單一主控台尋找規避個別端點產品的威脅。只要按一下按鈕，Symantec™ Advanced Threat Protection 就會在整個企業中搜尋、探索並矯正攻擊元件，無需新的端點代理程式。

[2] 賽門鐵克™ 2015 年 4 月出版之第 20 期網路安全威脅研究報告

重要功能與效益

- 結合了來自全球大型網路威脅情報網路的全球遙測與本地客戶的環境，掌握端點上原本可能規避偵測的攻擊。
- 按一下按鈕就可以搜尋、探索和矯正您企業中所有端點的任何攻擊跡象。
- 運用現有已安裝的 Symantec Endpoint Protection 產品，無需新的端點代理程式
- 整合 Symantec™ Advanced Threat Protection: Network、賽門鐵克™ 電子郵件安全雲端服務和 Symantec™ Advanced Threat Protection: Email，可跨控制點取得完整的能見度並矯正進階攻擊。

利用賽門鐵克服務讓您的資安處於最佳狀態、將風險降至最低並且獲得最高的投資報酬

聯繫賽門鐵克最有經驗的安全專家，他們能為您提供進階威脅防護訓練、主動規劃和風險管理，以及為您的企業進行部署、組態設定和評估解決方案。如需更多資訊，請造訪服務頁面：http://go.symantec.com/services

系統需求

適用於此使用者介面的瀏覽器用戶端

Microsoft Internet Explorer 11 或更高版本
Mozilla Firefox 26 或更新版本
Google Chrome 32 或更新版本

虛擬硬體裝置部署方式

VMware® ESXi 5.5、6.0
啟用 Intel 虛擬技術

虛擬機器 (Virtual Machine，簡稱 VM) 需求

- 四核心處理器 (實體或邏輯)
- 至少 32 GB 的記憶體
- 至少 500 GB 的磁碟空間
- VMFS-5 資料儲存區；或最少具有 2 MB 區塊大小的 VMFS-3。

實體硬體裝置部署方式

	硬體裝置型號 8840	**硬體裝置型號 8880**
外型尺寸	1U 高機架型	2U 高機架型
處理器	單一 Intel Xeon 六核心處理器	2 個 12 核心 Intel Xeon 處理器
記憶體	32 GB	96 GB
硬碟	1 台 1TB 硬碟	4 台 300GB RAID 5 硬碟
電源供應器	非備援式電源供應器 (PSU)	2 台 750W 備援電源供應器
網路介面卡	四個 Gigabit 乙太網路連接埠：	四個 10 Gigabit 乙太網路連接埠 二個 1 Gigabit 乙太網路連接埠
	1 組 WAN / LAN 1 個管理連接埠 1 個監控連接埠	2 組 WAN / LAN (10GB) 1 個管理連接埠 (1GB) 1 個監控連接埠 (1GB)

更多資訊

請造訪我們的網站

http://www.symantec.com/advanced-threat-protection

關於賽門鐵克

賽門鐵克保護全世界的資訊，也是安全、備份與可用性解決方案的全球領導廠商。我們創新的產品與服務能保護任何環境的人員與資訊，從最小的行動裝置到企業資料中心，乃至於雲端系統。我們在保護資料、身分與互動方面領先產業的專業能力，讓我們的客戶在連線世界中充滿信心。如需更多資訊，請造訪 www.symantec.com/zh/tw。

台灣賽門鐵克股份有限公司

地址：台北市信義路五段 7 號台北 101 大樓 13 樓 A 室
電話：(02) 8726-2000
傳真：(02) 8726-2199
www.symantec.com/zh/tw

21356813-2 10/15